Sheet # 2

Symmetric-Key Cryptography

Review Questions

1. In symmetric-key cryptography, how many keys are needed if Alice and Bob want to communicate with each other?
2. In symmetric-key cryptography, can Alice use the same key to communicate with both Bob and John? Explain your answer
3. In symmetric-key cryptography, if every person in a group of 10 people needs to communicate with every other person in another group of 10 people, how many secret keys are needed?
4. In symmetric-key cryptography, if e very person in a group of 10 people needs to communicate with every other person in the group, how many secret keys are needed?

Exercises

1. Using the Caesar cipher, encrypt the message "**attack at dawn**".

2. Decrypt the ciphertext "**LFDPH LVDZL FRQTX HUHG**" that has been encrypted using the Caesar cipher.

3. ***(Report)*** Encrypt the message "**this is an exercize**" using a shift cipher with a key of 20. Decrypt the message to get the original plain text.

4. Can we use mono-alphabetic substitution if our symbols are just 0 and 1? Is it a good idea? Repeat for the ploy-alphabetic case.

5. Encrypt the message "**surrender immediately**" using the affine transformation:

   $$C \equiv (11*P + 18) \bmod 26.$$

6. Decrypt the ciphertext "**RTOLK TOIK**", which was encrypted using the affine transformation: $C \equiv (3*P + 24) \bmod 26$.

7. If Q is the most common letter in a long ciphertext encrypted by a shift cipher:

   $$C \equiv (P + k) \bmod 26$$

   , what is the most likely value of k?

8. If W and B are the two most common letters in a long ciphertext, respectively encrypted by an affine transformation: $C \equiv (a*P + b) \bmod 26$

   , what are the most likely values for a and b?

9. Given two ciphers, plaintext may be encrypted by using one of the ciphers and then using the other cipher. This procedure produces a product cipher.

   a) Find the product cipher obtained by using the transformation

   $$C \equiv (5*P + 13) \bmod 26$$

   followed by the transformation $C \equiv (17*P + 3) \bmod 26$.

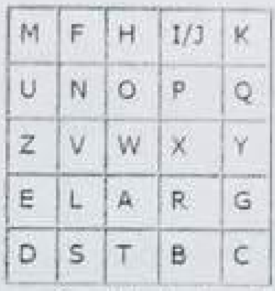
   b) Find the product cipher obtained by using the transformation

   $C \equiv (a*P + b) \bmod 26$ followed by the transformation

   $C \equiv (c*P + d) \bmod 26$, where $\gcd(a, 26) = \gcd(c, 26) = 1$.

10. For the ***Playfair*** cipher:

    a) Using the matrix below, Encrypt: "Must see you over Cadogan West. Coming at once."



M	F	H	I/J	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

    b) Repeat using the matrix with the key "largest"

    c) *(Report)* Repeat using the matrix with the key "Occurrence"

    d) *(Report)* Try decrypting the cipher again in one case to get the original message.

11. Encrypt the word: **renaissance** using a cipher that replaces each character with position a (A has a=0, B has a=1, ... etc.) by another character with position $f(a)=(a+k_i) \bmod n$. (n= 26 and K_i is equal to 0 for the 1st character, 17 for the 2nd, and 19 for the 3rd and then K_i is repeated 0,17,19,0,17,19,...etc). What is the type of this cipher?

12. With ***Vignere*** cipher and a key word "**secret**", encrypt the message "**do not open this envelope**".

13. ***(Report)*** Decrypt the ciphertext "WBRCSL AZGJMG KMFV", using previous ***Vignere*** cipher.

14. Decipher the following ciphertext, which was enciphered using a ***Vigenere cipher*** with key ART:

    YFN GFM IKK IXA T

15. Encrypt the sentence "**meet me after the toga party**" with a ***rail fence*** cipher of depth 2.

16. Encrypt "**INTERNET**" using a transposition cipher with the following keys:

a) The key:

3 5 2 1 4
1 2 3 4 5

b) The key is given by the word: **money**

17. Rotate **111001** three bits to the right.

18. Rotate **100111** three bits to the left.

19. A 6-by-2 S-box adds bits at odd-numbered positions (1, 3, 5) to get the right bit of the output and adds bits at even-numbered positions (2, 4, 6). If the input is **110010**, what is the output? If the input is **101101**, what is the output? Assume the rightmost bit is 1.

20. The left most bit of a 4-by-3 S-box rotates the other 3 bits. If the left most bit is 0, the 3 other bits are rotated to the right 1 bit. If the left most bit is 1, the 3 other bits are rotated to the left 1 bit. If the input is 1011, what is the output? If the input is **0110**, what is the output?

21. A P-box uses the following table for encryption. Show the box and connect the input to the output.

4 2 3 1
1 2

Is the P-box straight, compression, or expansion.

22. Compute the bits number 1, 16, 33, and 48 at the output of the *first round of the DES **decryption***, assuming that the cipher text is composed of all ones and the external key is composed of all zeros, and that all the S-boxes are 6-by-4 that takes the *middle 4 bits* from the 6- bit input.

23. A message with two blocks P_0 and P_1 is encrypted using the ***CBC mode*** and the encryption technique was *rotation 3 bits to the right.* The resultant ciphers C_0 and C_1 were 11001100 and 00010001 respectively. If the IV=11111111, what were the blocks P_0 and P_1?

Best Wishes of Success